GLOSSARY OF TECHNICAL TERMS

BIG i AGENTS COUNCIL FOR TECHNOLOGY.

Artificial Intelligence (AI)

The simulation of human intelligence processes by machines, including learning, reasoning, and self-correction.

Bias in AI

Systematic errors in AI outputs caused by biased training data or flawed algorithms, which can lead to unfair or inaccurate results.

Encryption in Transit and at Rest

Encryption in transit protects data while it is being transmitted. Encryption at rest protects data stored on a device or server.

Explainability

The degree to which an AI system's decisions can be understood and interpreted by humans.

Generative AI

AI that can create new content such as text, images, or music based on training data.

GLBA

Gramm-Leach-Bliley Act, a U.S. law that requires financial institutions to explain how they share and protect customers' private information.

HIPAA

Health Insurance Portability and Accountability Act, a U.S. law that protects sensitive patient health information.

Inference

The process of using a trained AI model to make predictions or generate outputs based on new input data.

ISO 27001

An international standard for managing information security.

Large Language Model (LLM)

A type of AI model trained on vast amounts of text data to understand and generate human-like language (e.g., ChatGPT, Claude).

Machine Learning (ML)

A subset of AI that enables systems to learn from data and improve performance over time without being explicitly programmed.

Model Hallucination

When an AI generates incorrect or fabricated information that appears plausible.

Natural Language Processing (NLP)

A branch of AI that helps computers understand, interpret, and generate human language.

Predictive AI

AI that analyzes data to make predictions about future outcomes.

Prompt Engineering

The practice of crafting effective inputs (prompts) to guide AI models toward desired outputs.

Rule-based AI

AI that operates based on a set of predefined rules and logic.

SLAs

Service Level Agreements, which define the level of service expected from a vendor, including uptime and response times.

SOC 2 Type II

A certification that evaluates an organization's information systems relevant to security, availability, processing integrity, confidentiality, and privacy over a period of time.

Training Data

The dataset used to teach an AI model how to perform tasks or make predictions.